IN THE CLAIMS:

Please amend claims 1-2, 4, 6-8, 10, 22-24, 46, 56, 58-60, and 62 as follows.

1.   (Currently Amended) An apparatus, comprising:

a determiner configured to determine whether a message received at a first network has been through a security check by determining whether or not the message has been received with security at a first layer;

a forwarder configured to forward the message within said first network regardless of the result of the determination; and

a modifier configured to modify the message so as to include a second layer indication that the message has not been through a security check ~~if~~ when the result of the determination is that the message has not been through a security check, wherein said second layer is a higher layer than said first layer.

2.   (Currently Amended) The apparatus according to claim 1, ~~wherein~~ further comprising:

~~the~~ a receiver ~~is~~ configured to receive messages via a secure interface and a second network and directly from outside the first network.

3.   (Cancelled)

4.   (Currently Amended) The apparatus according to claim 1, wherein the message ~~includes~~ comprises a second layer identity header, and wherein the modifier is configured to include said second layer indication in said second layer identity header of the message.

5.   (Previously Presented) The apparatus according to claim 4, wherein the message comprises a session initiation protocol message.

6.   (Currently Amended) The apparatus according to claim 4, wherein the identity header comprises a ~~P-Asserted-Identity~~p-asserted identity.

7.   (Currently Amended) The apparatus according to claim 1, wherein the message ~~includes~~ comprises a second layer identity header, and wherein the modifier is further configured to modify the message so as to indicate that the message has not been through a security check by removing at least part of the second layer identity header.

8.   (Currently Amended) The apparatus according to claim 7, further comprising:

    a detector configured to detect whether the second layer identity header is of a particular type and ~~if~~when so to remove at least part of the header.

Application No.: 10/614,343

9.   (Previously Presented) The apparatus according to claim 7, wherein the message comprises a session initiation protocol message.

10.   (Currently Amended) The apparatus according to claim 8, wherein the detector is configured to detect whether the second layer identity header comprises a ~~P-Asserted-Identity~~p-asserted identity ~~type~~.

11.   (Cancelled)

12.   (Cancelled)

13.   (Previously Presented) The apparatus according to claim 1, wherein the apparatus comprises an interrogating call session control function.

14. - 21. (Cancelled)

22.   (Currently Amended) A system, comprising:

a security server; and

a network processing element, the security server being configured to receive a message, determine whether the message has been through a security check by determining whether or not the message has been received with security at a first layer, ~~if~~

Application No.: 10/614,343

when the result of the determination is that the message has not been through a security check modify the message so as to include a second layer indication that the message has not been through a security check, wherein said second layer is a higher layer than said first layer, and forward the message to the network processing element regardless of the result of the determination.

23.   (Currently Amended) The system according to claim 22, wherein the security server is configured to receive messages via a secure interface and another security domain and directly from outside the system.

24.   (Currently Amended) The system according to claim 22, wherein the network processing element is configured to,

receive a message forwarded by the security server, and

determine whether the message has been modified so as to include a second layer indication that the message has not been through a security check, and, if when the message has been so modified, perform one or more security checks in respect of the message.

25.   (Previously Presented) A method, comprising:

determining that a message received at a first network has not been through a security check by determining that the message has not been received with security at a first layer;

modifying the message so as to include a second layer indication that the message has not been through a security check, wherein the second layer is a higher layer than the first layer; and

forwarding the message within the first network.

26.-45. (Cancelled)

46.   (Currently Amended) An apparatus, comprising:

determining means for determining whether a message received at a first network has been through a security check by determining whether or not the message has been received with security at a first layer;

modifying means for, if when the message is determined not to have been through a security check, modifying the message to include a second layer indication that the message has not been through a security check, wherein the second layer is a higher layer than the first layer; and

forwarding means for forwarding the message within the telecommunications network regardless of whether the message has been through a security check.

Application No.: 10/614,343

47.-55. (Cancelled)

56. (Currently Amended) The method according to claim 25, wherein the message ~~includes~~ comprises a second layer identity header, and comprising including said second layer indication in said second layer identity header of the message.

57. (Previously Presented) The method according to claim 56, wherein the message comprises a session initiation protocol message.

58. (Currently Amended) The method according to claim 56, wherein the identity header comprises a ~~P-Asserted-Identity~~p-asserted identity.

59. (Currently Amended) The method according to claim 25, wherein the message comprises~~includes~~ a second layer identity header, and further comprising:

modifying the message so as to include a second layer indication that the message has not been through a security check by removing at least part of the second layer identity header.

60. (Currently Amended) The method according to claim 25, further comprising:

detecting whether the second layer identity header is of a particular type and ~~if~~ when so removing at least part of the header.

61.   (Previously Presented) The method according to claim 60, wherein the message comprises a session initiation protocol message.

62.   (Currently Amended) The method according to claim 61, further comprising:

detecting whether the second layer identity header comprises a ~~P-Asserted-Identity~~p-asserted identity type.

63.   (Previously Presented) The apparatus according to claim 1, wherein said security at a first layer is security applied to a message at a secure interface between two security domains.

64.   (Previously Presented) The apparatus according to claim 63, wherein said secure interface is a Za interface.

65.   (Previously Presented) The apparatus according to claim 1, wherein said forwarder is configured to forward said message over a Zb interface.

66.   (Previously Presented) The system according to claim 1, wherein said security at a first layer is security applied to a message at a secure interface between two security domains.

Application No.: 10/614,343

67.   (Previously Presented)   The system according to claim 66, wherein said secure interface is a Za interface.

68.   (Previously Presented)   The system according to claim 22, wherein said security server is configured to forward said message to said network processing element over a Zb interface.

69.   (Previously Presented)   The method according to claim 25, wherein said security at a first layer is security applied to a message at a secure interface between two security domains.

70.   (Previously Presented)   The method according to claim 69, wherein said secure interface is a Za interface.

71.   (Previously Presented)   The method according to claim 25, comprising forwarding said message within said first network over a Zb interface.

Application No.: 10/614,343